K7 SECURITY

Cyber Threat Monitor Report

Q2_2021-22

www.k7computing.com

Contents

A Glimpse into the Cyber Threat World

Even after the continuous plunge in the number of recorded cases worldwide, the dreadful Covid-19 is not over yet. The glimpse of light at the end of the tunnel, so to speak, is the growing awareness among global citizens to combat the SARS-CoV-2 strain by getting vaccinated and following the prescribed safety protocols. We wish the same could happen among the netizens concerning digital hygiene.

Despite several warnings and words of caution by the cybersecurity solution providers, a significant part of the netizens are still casual about basic cyber hygiene practices. Unfortunately, similar ignorance is practiced by innumerable SMEs, SOHOs, and startups. And even worse, many of them still do not seem to understand the probable loss they could bear if a threat actor successfully victimised them.

This can be seen from the fact that some of them still use dated systems such as using Windows 7 or Windows 8 powered computers for industrial productions. One of the primary reasons why they fail to shift to more secure versions is that some of their application software is supported only on these operating system versions and their software is yet to be updated. Unfortunately, both these software providers and their consumers misjudge the severity, and thus unknowingly invite malware attacks.

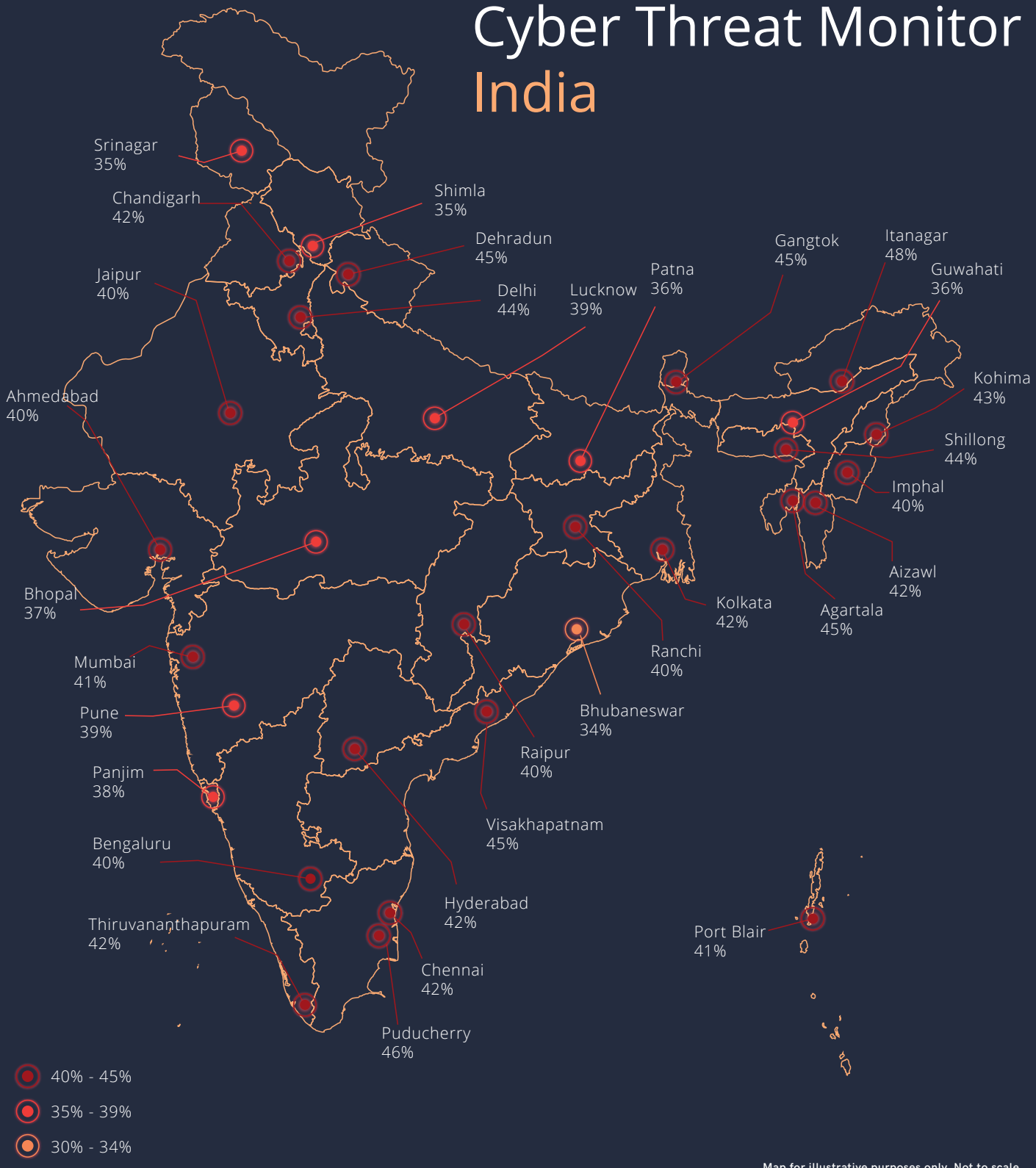
In the past three months, our researchers uncovered hundreds and thousands of thwarted attacks inside and outside the country. Interestingly, a significant part of these attacks were due to unpatched old vulnerabilities such as SMBV3.

In this era of unprecedented uncertainty, countering such risks requires a cooperative effort involving end-users and enterprises alike. That is perhaps the only way to strengthen the bond between the security providers and the consumers to manage risks effectively. It's time to take the first step towards this initiative.

Happy reading, stay safe and stay healthy!

We would appreciate you sharing this report among your colleagues and friends to raise awareness of the prevalence of cyber threats, thus helping to make the digital world a safer place!

Cyber Threat Monitor
India



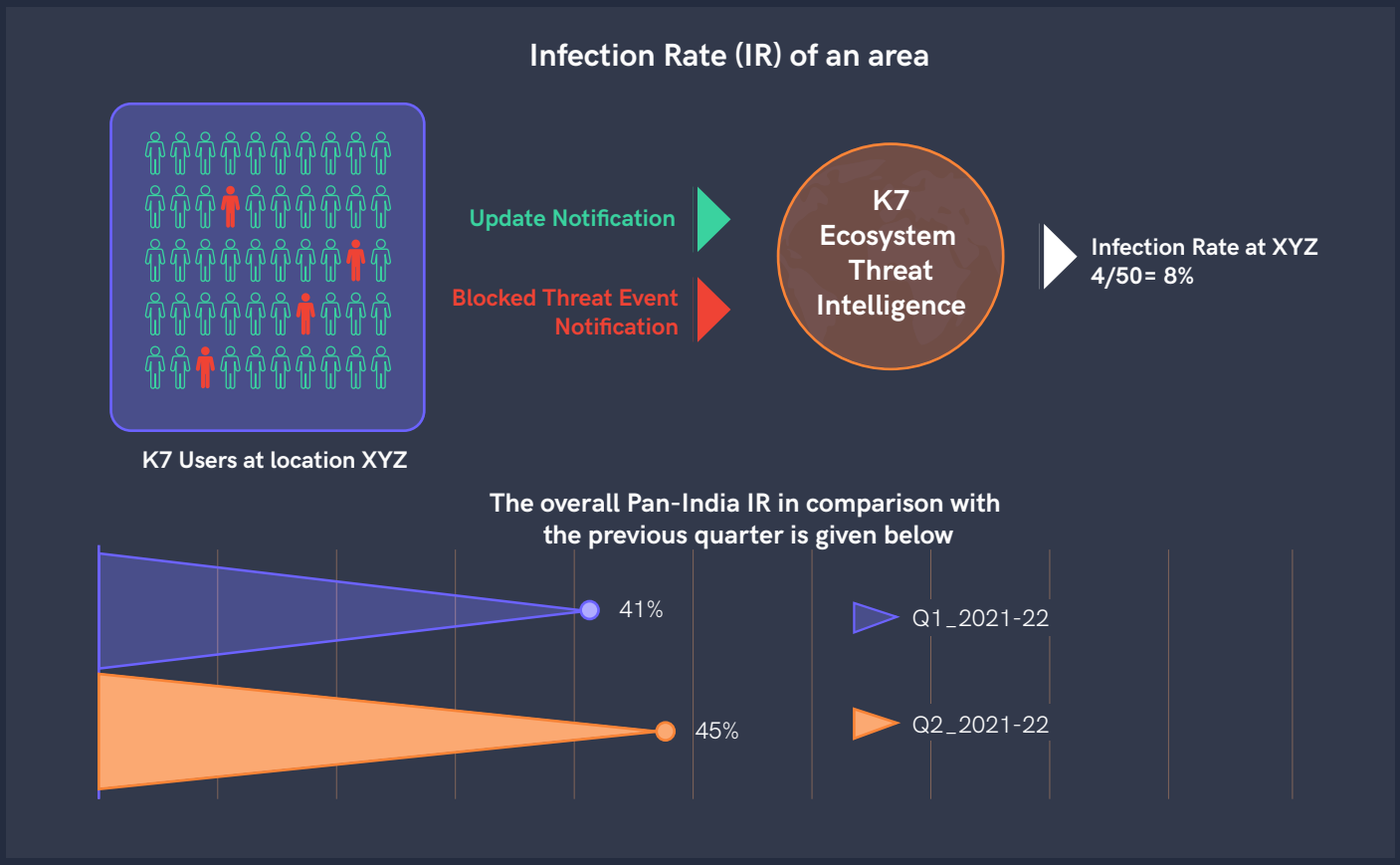
Map for illustrative purposes only. Not to scale.

Back to contents

Regional Infection Profile

Over 30 years, K7 Computing has successfully safeguarded millions of clients globally from various cyber threats. The cyber threat monitor report offers a snapshot of the threats observed during each quarter.

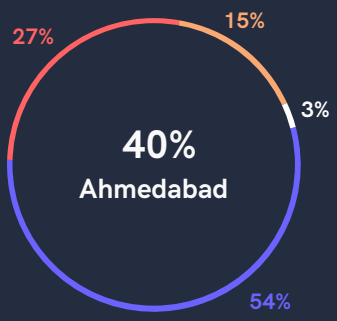
To better understand the present condition of the domestic threat landscape, we have designed a concept called Infection Rate (IR). The idea is picturised as follows.

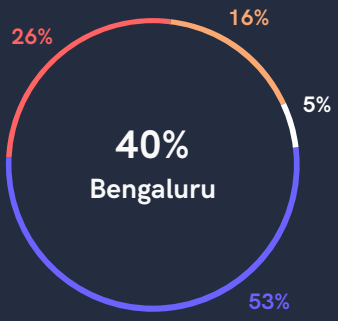


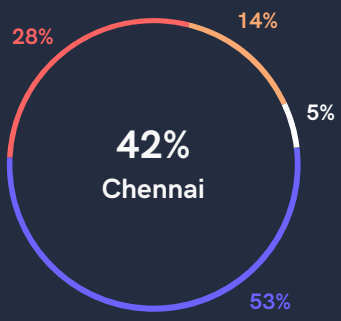
The sustained steady escalation of infection rate around the country has become a standard for many years. This quarter was no exception either.

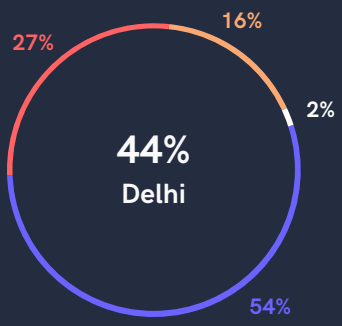
The threat type breakdown for the Windows OS across Metros and Tier-1 cities is as depicted below.

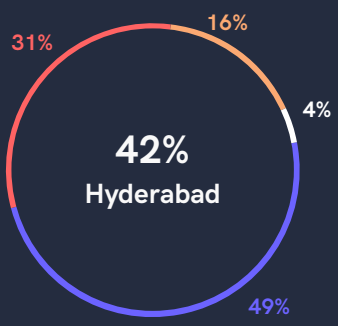
The Metros and Tier - 1 Cities - Infection Rate

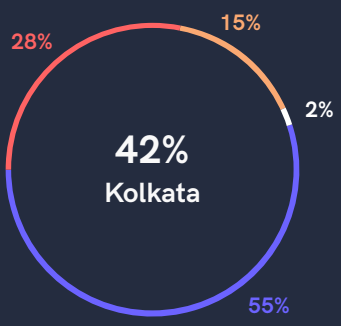


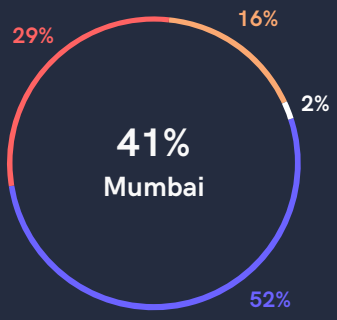


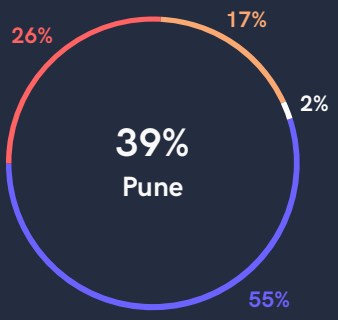








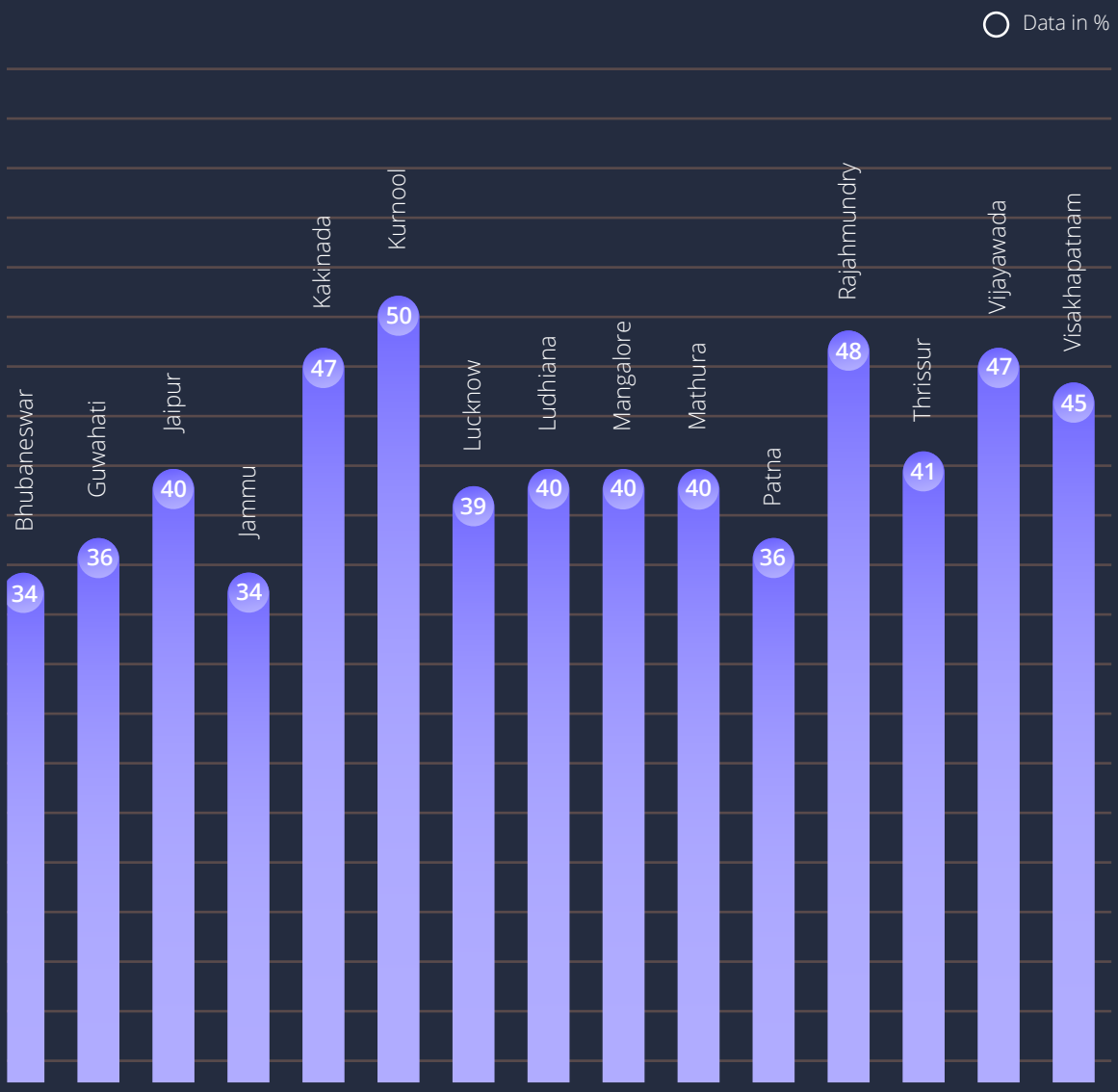




Behaviour Protection Firewall Protection ScanEngine Protection Web Protection

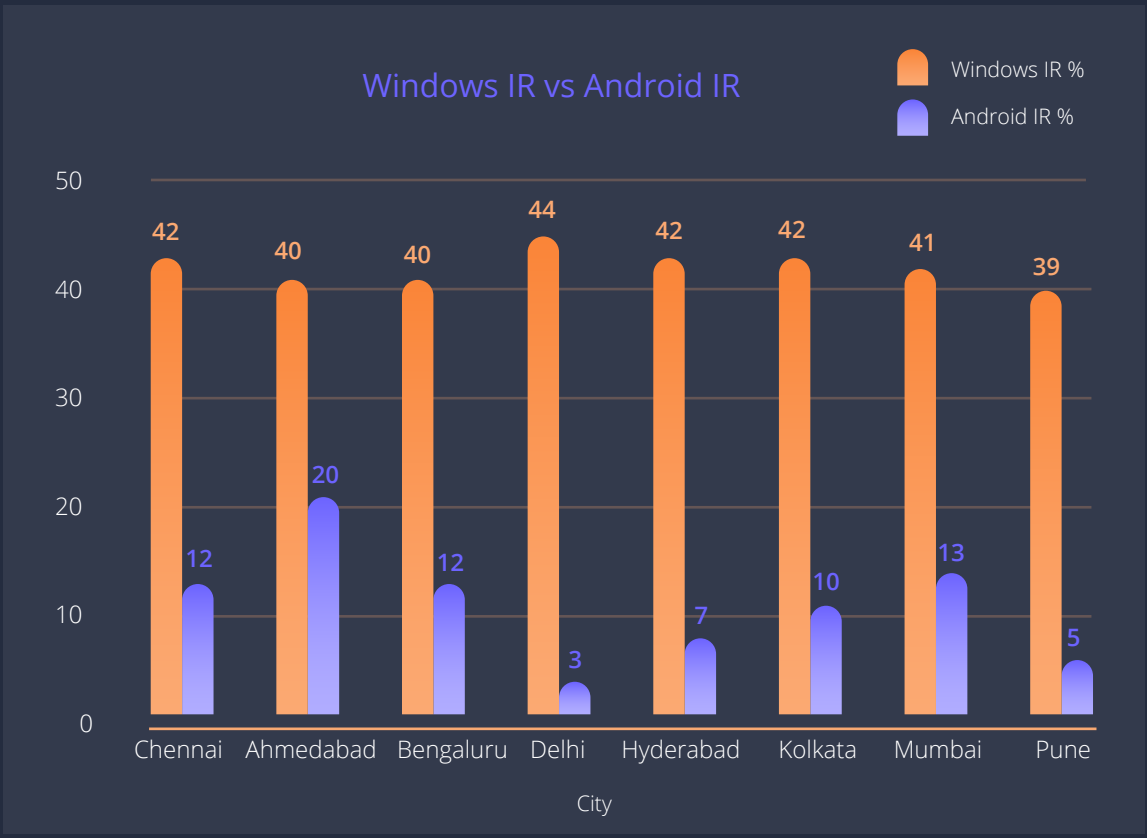
Tier-2 cities are also facing an increase in threats as shown in the proportion of thwarted attacks.

Top 15 Infection Rates in Tier - 2 Cities



Infection Rate Comparison across Platforms

In spite of the popularity of the Windows platform, Android-powered devices are rapidly becoming the primary choice among many users for regular activities. As more and more users are preferring mobiles over desktops, we at K7 Labs have included a separate Android IR, along with comparing the threat scenario between Windows and Android devices in this report. Let's see what has been reported to our rich K7 Ecosystem Threat Intelligence (K7ETI) infrastructure. Android OS, albeit with its own flaws, is projected to be more secure than Windows as it has been designed this way from a security aspect when compared with its desktop counterparts. For example, Google has stringent vetting procedures for apps uploaded on its Play Store, where it also ensures that non-Play Store apps are not typically executable by default, making the environment more controlled, which in turn makes the mobile experience more secure. The IR graph depicted below complements what has been mentioned earlier.



Though statistics alone aren't sufficient to explain the threat environment, it did, however, give us the likely trends in which the threat environment is swaying. From the statistics, we can see that smart cities are definitely not smart enough to protect themselves from the threat actors. Threat actors play it safe to lure gullible victims. Work From Home, the usage of BYOD and lack of employee cybersecurity training, especially during the pandemic, have added to the rise in attacks. Organizations should ensure safe cyber security practices and regular training on the latest cyber threats, for example the comprehensive Cyber Awareness training course delivered by our K7 Academy, to combat this.

The detailed threat scenario of this quarter is explained in the separate sections below.

Enterprise Insecurity

Irrespective of whether an organization is a large enterprise, an SME or a startup, there's no dearth of cyber security issues for them. To make their tradecraft more effective, threat actors embrace new techniques, including exploiting latest vulnerabilities and manipulating leaked credentials thereby continually transforming the threat landscape, leading us to an increasingly complex digital ecosystem.

We don't have to look far into the past to see how the threat actors are propelling new attack methods. For example, in the second quarter of the financial year 2021-22, there were two significant incidents at our enterprise clients premises which have been illustrated below.

Case Study 1: Lemon Duck Miner Wreaking Havoc

During a recent escalation, we came across a network with systems having multiple scheduled tasks. On further analysis, it was found that this was the **"Lemon Duck"** malware that creates and executes malicious scheduled tasks and scripts. The infection chain is as illustrated below:

Case Study 2: Adhubllka Brute Forcing itself into Unsecured Devices

In another noticeable instance, an enterprise network was infected with Adhubllka ransomware. Interestingly, the ransomware encrypted only the files on one of the secondary partitions and left the system folders, installed software and the rest unencrypted.

Here is how the ransomware accomplished its mission:

01

Attackers brute forced via RDP onto the unprotected system and executed the ransomware

02

All the local files on the infected system and folders shared with it were encrypted

03

This resulted in multiple systems whose files and drives were shared with the infected system being encrypted even without the ransomware actually running on those systems

Safety Recommendations

- Administrators should restrict RDP to known, trusted IPs and changing its default port
- Keep all your devices, including your OS, updated and patched against latest vulnerabilities
- ALL systems in the network should have a reputable enterprise security suite, such as K7 Endpoint Security, installed and kept updated

Vulnerabilities Galore

Software glitches, popularly known as vulnerabilities, are the most important highlight of any threat landscape. Vulnerabilities are like threat actor magnets, as they usually offer an initial foothold on the targeted devices. And once an adversary gains access, they can further exploit them by executing malicious payloads and/or propagating across the network.

An innumerable availability of new and old vulnerabilities in various software and hardware environments results in a burgeoning of daily attacks, most of which belongs to the enterprise software and hardware systems,

Highlighting all these vulnerabilities individually is beyond the scope of this periodic report; however, we have handpicked the most pervasive ones we encountered in the last quarter, and have given a brief on them in this section (in no particular order).

RCE Vulnerability in Windows Printer Spooler

CVE-2021-34527, aka "Printer Nightmare", is a remote code execution (RCE) vulnerability in Windows Printer Spooler service. **CVE-2021-36936**, is another RCE vulnerability in the printer spooler service.

The vulnerable Windows versions are Windows 7, Windows 8.1, Windows 10, Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016, 2019, 2004 and 20H2.

Users are advised to install the patch(es) issued by Microsoft for these vulnerabilities and disable the printer spooler service if not needed.

Vulnerability in Kaseya VSA

Kaseya made global news in the last quarter due to a widespread ransomware attack as a result of **CVE-2021-30116** in its Kaseya Virtual System/Server Administrator (VSA) servers which allowed adversaries to control VSA and deploy ransomware in Kaseya's customer environment.

The vulnerable versions are the Kaseya VSA platforms before v9.5.7a.

Kaseya released a detection tool "**Kaseya VSA detection tool**" to check if the system is exploited through this zero day vulnerability. Users are advised to patch their VSA systems.

Windows DNS Server RCE Vulnerability

CVE-2021-34494 is an RCE vulnerability in DNS affecting all Windows DNS servers from version 2008. This is a high risk vulnerability as it requires zero interaction from the user to achieve RCE.

Critical Vulnerability in Microsoft's Trident Engine

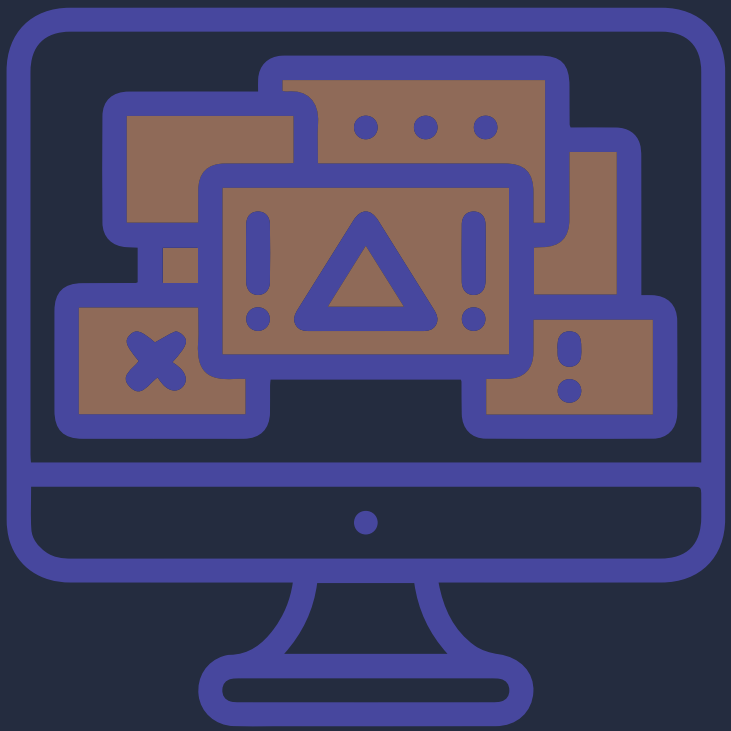
CVE-2021-40444 is an RCE vulnerability in Windows MSHTML engine which could be exploited by attackers to trick users into opening specially crafted Microsoft Office documents containing malicious ActiveX control.

The vulnerable Windows versions are Windows 10, Windows Server 2019, Windows Server 2016, Windows 7, Windows 8.1, Windows Server 2008 and Windows Server 2012.

SonicWall Products Affected by Buffer Overflow Vulnerability

CVE-2021-20019, a buffer overflow in HTTP Request Header leads to partial memory leak and causes DoS or arbitrary code execution The vulnerability lies in the web page of VPN and product management products such as NSa, TZ (GEN7)NSa,TZ- 7.0.1-713 and older; NSsp (GEN7)NSsp- below <7.0.0.376; NSv (Virtual: VMWare/Hyper-V/AWS/Azure/KVM) SonicOSv - 6.5.4.4-44v-21-955 and older.

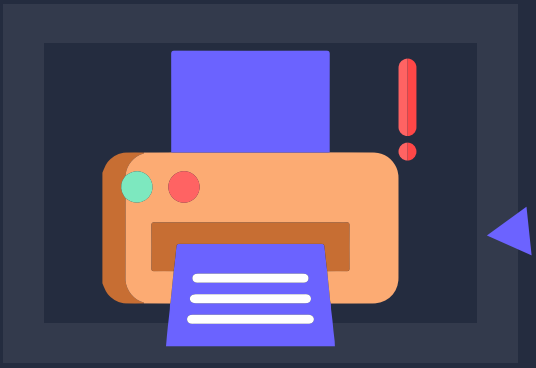
Users are strictly advised to patch the SonicOS at the earliest.



Danger in the Internet Of Things

In tandem with how the usage of IoT devices surged across enterprises and consumers alike, the vulnerabilities in these devices too are brimming with flaws. The perpetual tide raises serious safety concerns around the IoT space.

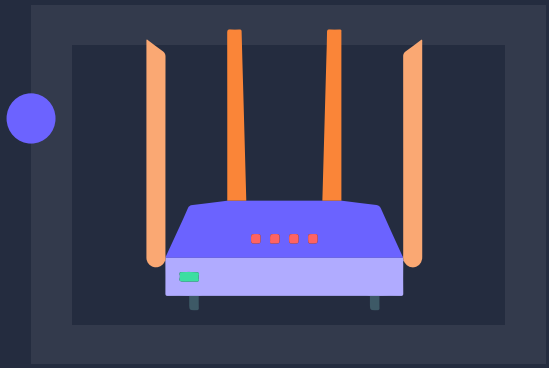
Here are the most concerning vulnerabilities from the colossal list.



Privilege Escalation Vulnerabilities in HP and Samsung Printers

CVE-2021-3438 is a privilege escalation vulnerability due to a buffer overflow in printer software drivers installed on Windows. The vulnerability is caused due to the improper implementation of code derived from Microsoft's Windows Driver Samples Project which contains insecure string copy functions, resulting in a buffer overflow.

Vulnerable devices are multiple HP LaserJet and Samsung printers (e.g. HP Color Laser 150 Series and Samsung CLP-360 Color Laser Printer series).



Vulnerabilities in NETGEAR Smart Switches

Demon's Cries is a vulnerability in Netgear switch's sccd daemon which implements the Netgear Switch Discovery Protocol (NSDP) on the switch. This vulnerability is a result of improper validation of "Set" requests' Type-Length-Value(TLV), which is used to update values on the device such as setting password, etc. in sccd daemon. An attacker can exploit this vulnerability allowing the attacker to change the device's admin password without knowing the previous password.

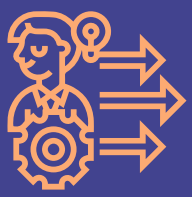
Draconian Fea is a race condition type vulnerability in Netgear switches with which an unauthenticated user can take over an authenticated session by spoofing the administrator's IP.

The vulnerable devices are GC108P, GC108PP, GS108Tv3, GS110TPP, GS110TPv3, GS110TUP, GS308T, GS310TP, GS710TUP, GS716TP, GS716TPP, GS724TPP, GS724TPv2, GS728TPPv2, GS728TPv2, GS750E, GS752TPP, GS752TPv2, MS510TXM and MS510TXUP.

Devices Exploitable by Zero-Click ForcedEntry

CVE-2021-30860 is an integer overflow vulnerability in CoreGraphics which on exploitation leads to possible arbitrary code execution. An attacker can exploit this vulnerability by tricking users into opening specially crafted PDF files.

The vulnerable versions are iOS 14.8, iPadOS 14.8, macOS Big Sur 11.6 and watchOS 7.6.2.



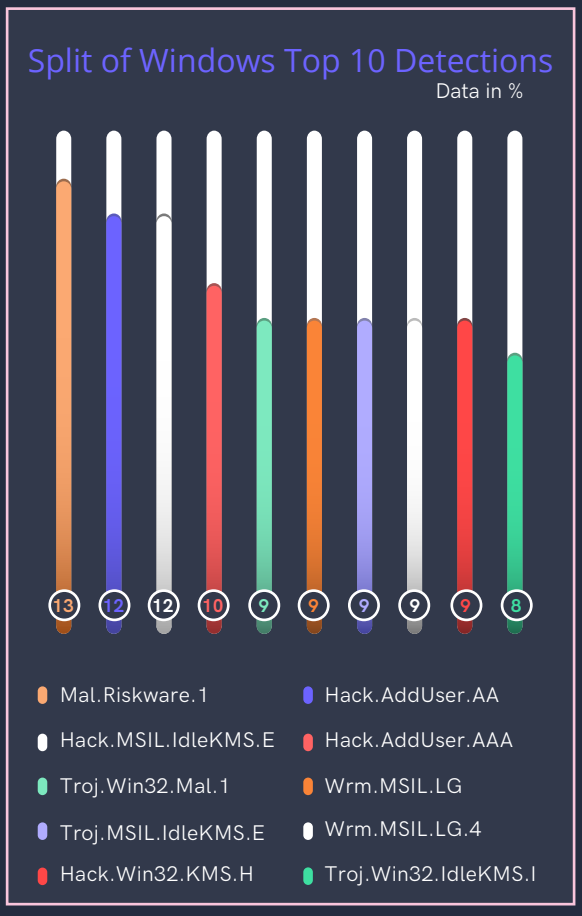
Mitigation Techniques

- Continuously monitor all IoT devices on your network and keep a track of their configurations
- Ensure all your devices are kept up to date and patched against the latest vulnerabilities

Windows Under Siege

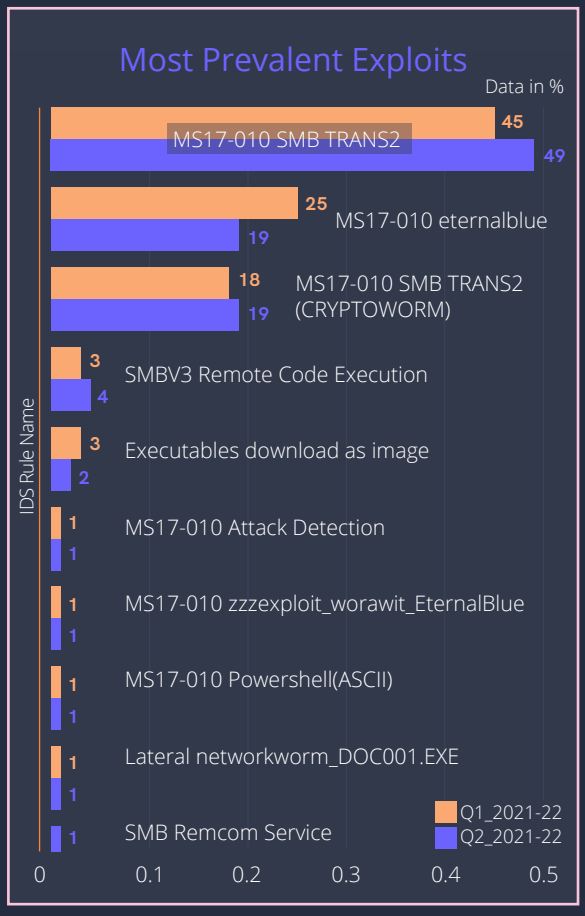
Windows Malware Type Breakdown

By all accounts, this quarter too remained quite challenging for Windows users across the country. The threat actors were operating malware throughout the period by toughening their delivery mechanism, triggering exploits and embracing various other obfuscation techniques. Let's look at what our telemetry reflected.



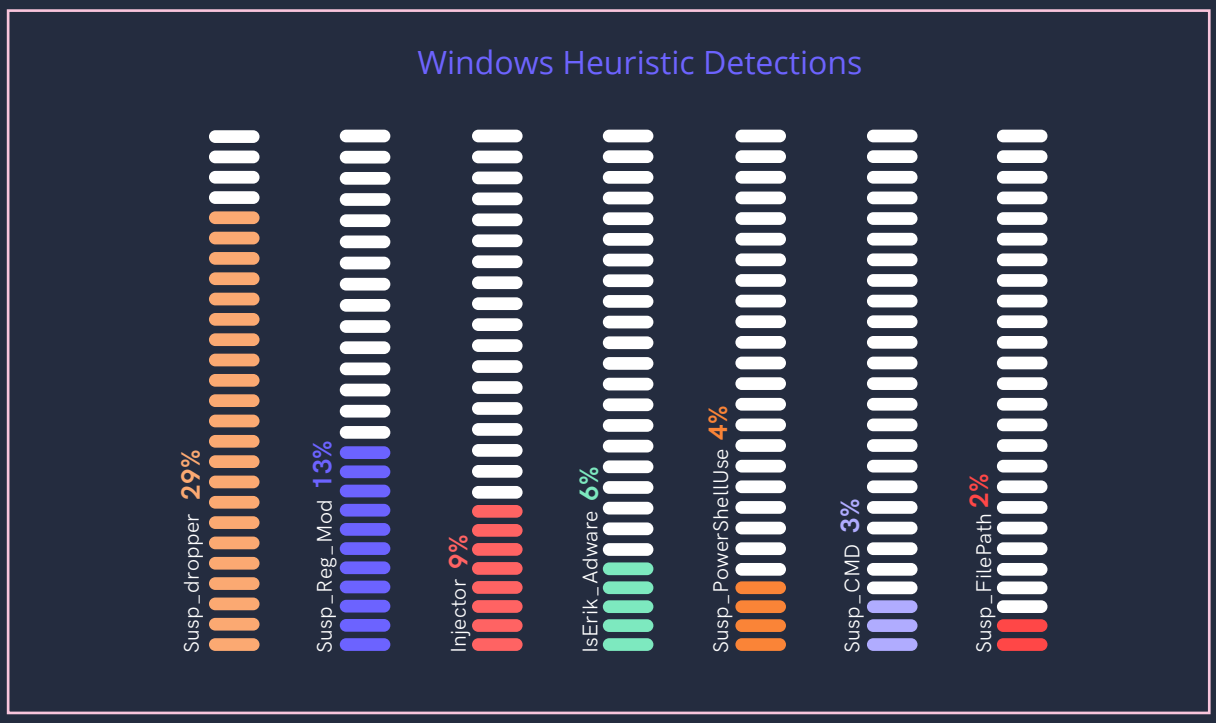
Windows Exploits

Despite several warnings and streams of cyber security headlines, many Windows users still prefer to leave their OS and installed software unpatched, resulting in a slew of vulnerable systems in the wild. The available exploits, such as SMB or PowerShell related exploits, help the threat actors in gaining initial access to devices or escalating privileges to gain control of the victim's system.



Host Intrusion Prevention System Heuristics

Our Host Intrusion Prevention System (HIPS) is a way of heuristically detecting threats based on their runtime behaviour. These are ideal for detecting new threats as well as newer variants of existing malware families. Let us see what our heuristic engine has detected in the last quarter.



Malicious droppers occupied a significant chunk followed by registry modifiers and code injectors. Our behavioural detection also identified malware that were hosted as malicious scripts on websites abusing PowerShell and Windows command shell. A small percentage of the detections were those of malware trying to evade detection by using suspicious file paths.

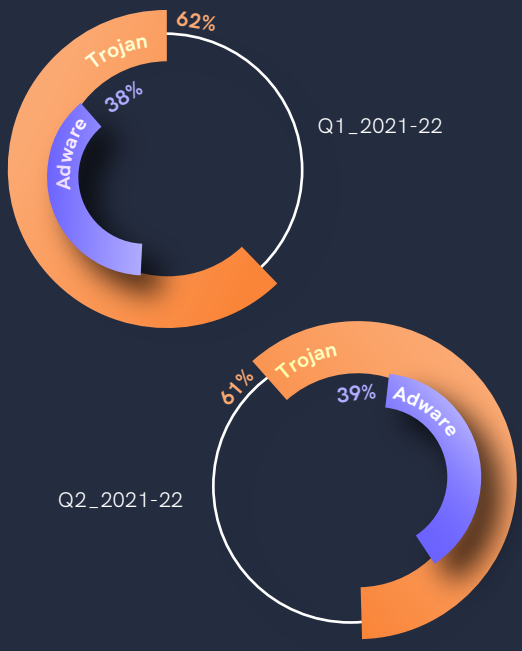
Mitigation Tips

- Keep your devices updated and patched against the latest vulnerabilities
- Follow the principle of least privilege while granting access to your employees
- Enforce a robust password policy

The Mobile Device Story

Malware attacks targeting Android users are increasing at a steep rate. Most of its threat landscape is shared by Trojans when compared with Adware.

Adware vs Trojan Proportional Split



In the last quarter, we once again see that adversaries around the world unfolded various tactics and techniques to accomplish their hostile intentions. The most popular mobile OS, Android, has endured large chunks of such attacks every day. For instance, Joker, the notorious Trojan, has spawned a barrage of attacks over this space.

Case Study: No Joking Around with JOKER

In the past few years, innumerable avatars of Joker popped on to the Google Play Store by adopting various tactics such as modifying chunks of code or payload downloading techniques to stay stealth. Recently we found its strains on a series of apps on the Google Play Store. Looking into one such malicious app, we discerned some exciting patterns in it.

The kill-chain of the latest version, which we observed recently, is as follows:

THE CAMOUFLAGE
Once launched, it retrieves the first level payload from a hardcoded URL, enabling the parent malware with additional capabilities

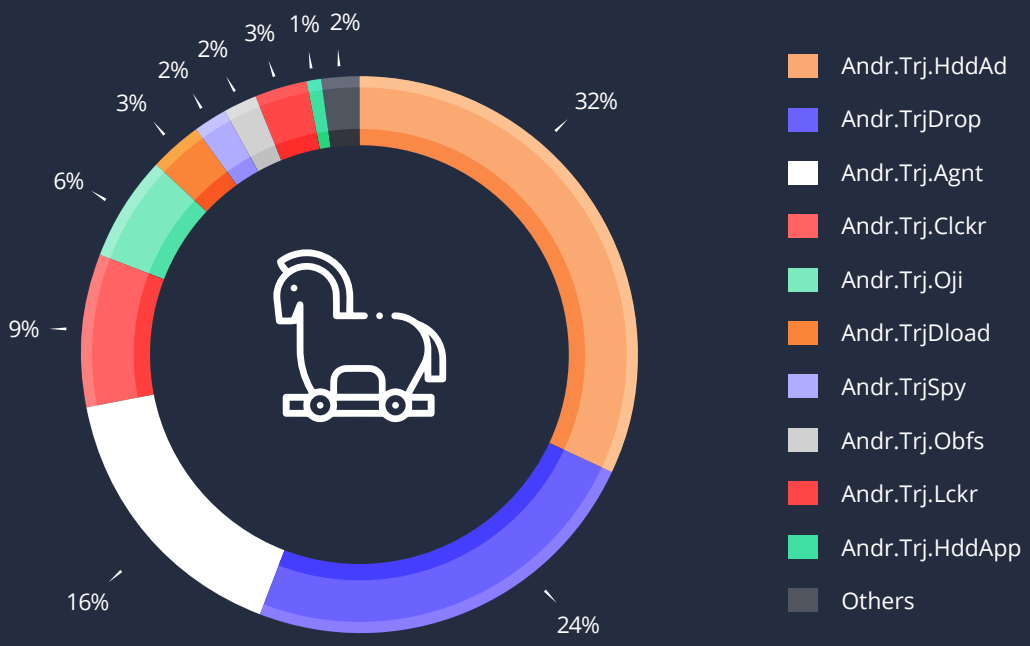
THE SHEPHERD
The first payload has a base64 encoded malicious URL to download the second payload

AND THE STRIFE BEGINS
The second payload installed is the Joker malware that attempts to intercept incoming SMS messages and subscribes to paid premium services

The Ubiquitous Trojan

Last quarter, many new Trojans were noticed in the Android threat landscape.

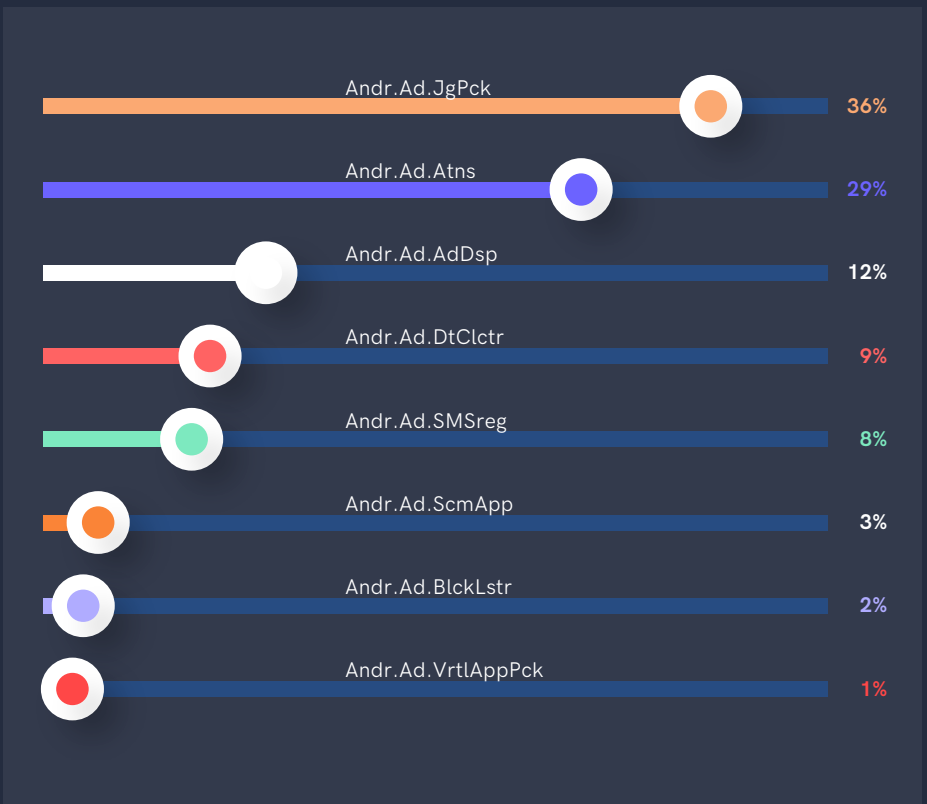
Most Prevalent Trojan Types



The Adware Impact

A detrimental bunch of adware bent on making quick and easy money remained omnipresent last quarter too. We noticed a plethora of adware, out of which the majority belong to older families, existing on Google's official app store as well as on third-party app stores.

Trend Line Showing the Adware Plague



Tips to Stay Safe

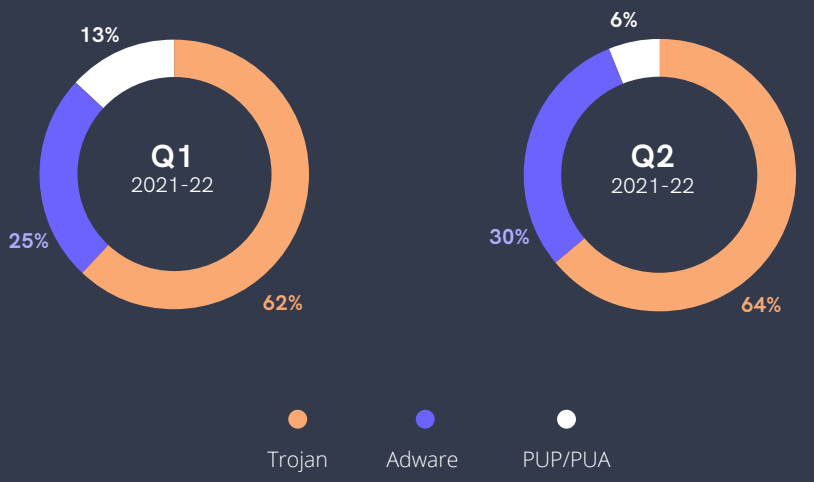
- Always be extra cautious when downloading and installing any app
- Do not download apps from unknown sources or third-party app stores
- Keep your OS and devices updated and patched against the latest vulnerabilities
- Install a robust security product like K7 Mobile Security to stay protected from the latest threats and update it regularly

Mac Attack

From the different Trojans, coin miners and ransomware variants that we noticed last quarter, we can glean that threat actors are also increasingly targeting macOS.

Though the proportion of PUPs on the macOS space has diminished considerably, threat actors are still not losing hope in raising their presence.

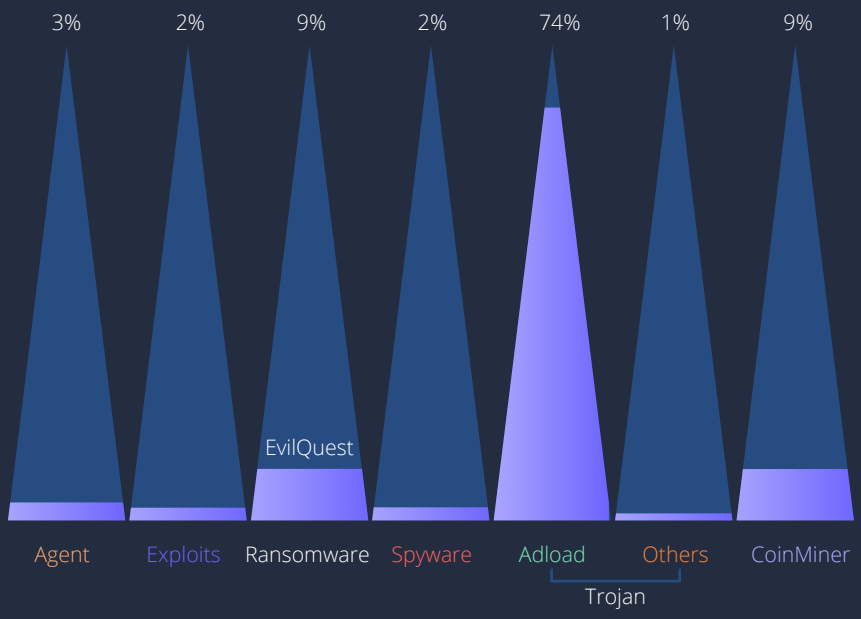
Trojan Adware & PUP Proportional Split



The Trojan Brouhaha

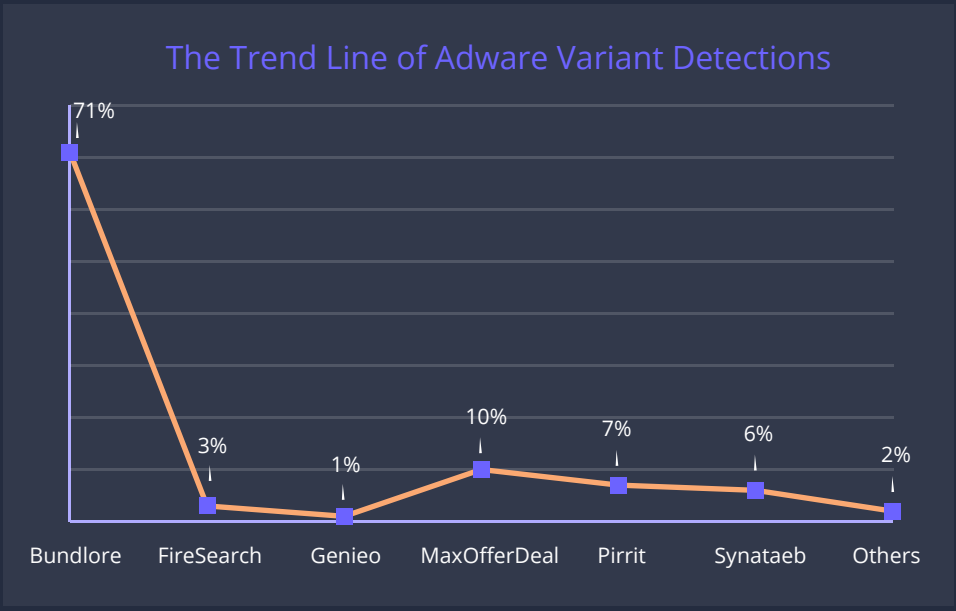
Notorious Trojans, such as Adload and EvilQuest ransomware, and some coin miners, continue to pose a severe threat, contributing to more than three-fourth of total Trojan attacks we thwarted this quarter.

Trojan Detection Trend Lines



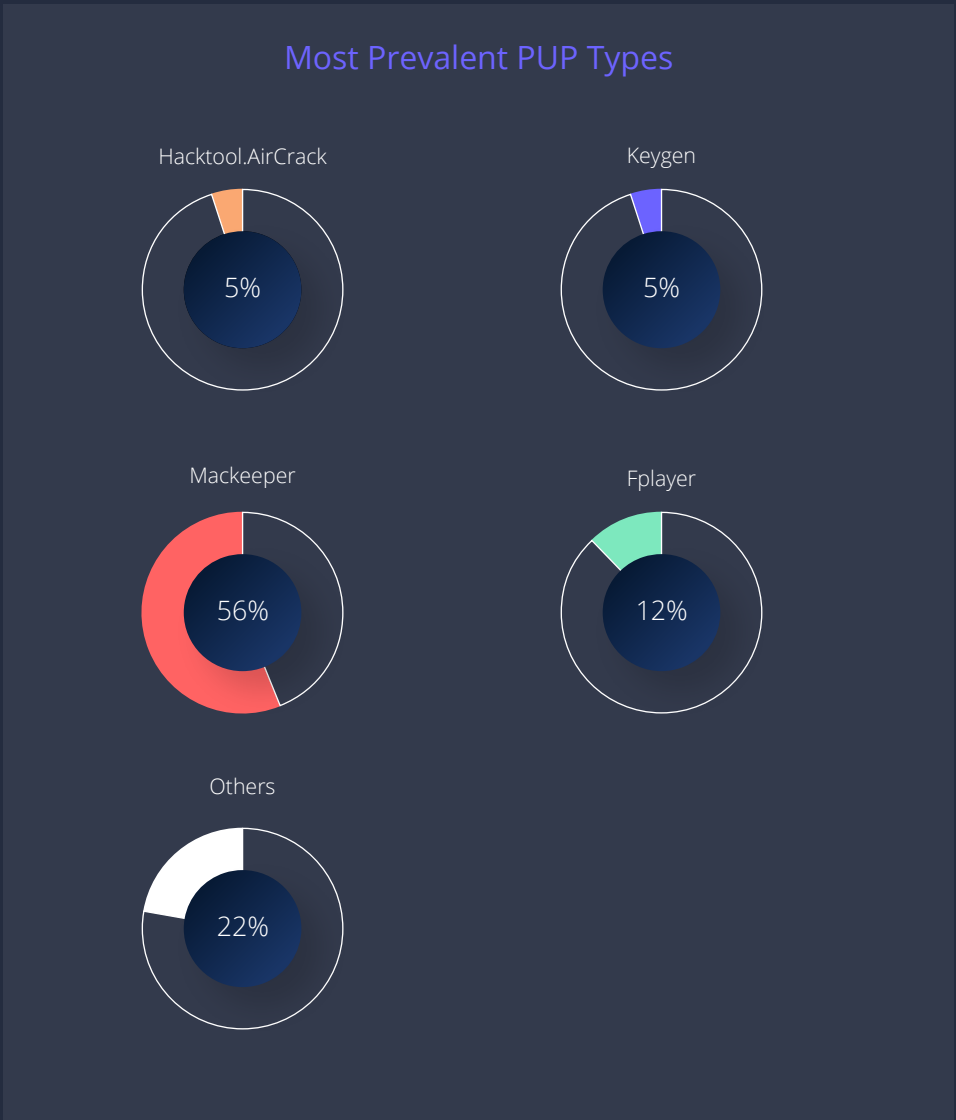
The Adware Saga

In the macOS space, the proportion of adware noticed each quarter is not very significant. This could be attributed to the strict reviewing policy of Apple. Despite that, the Bundlore adware variant is still quite prevalent in the macOS space.



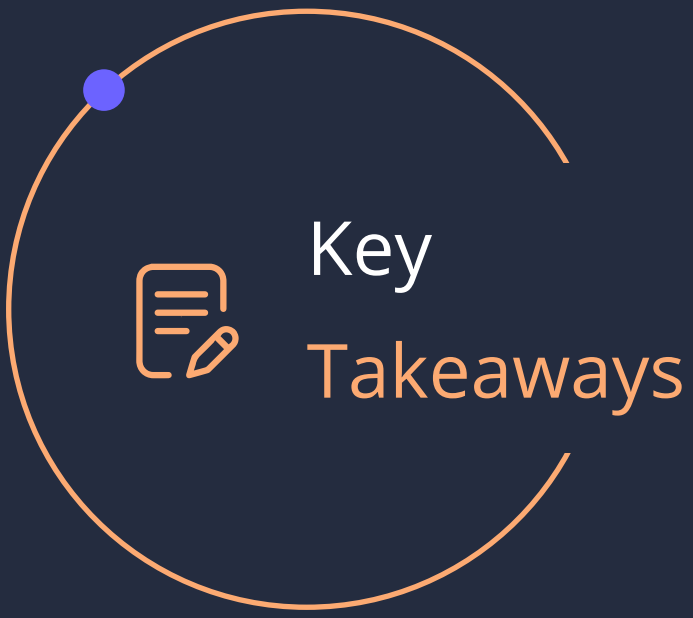
A Trickle of PUPs

The PUPs tracked last quarter are much less in comparison to Trojan and adware. The most significant among them were Mackeeper and Fplayer.



Safety Guidelines

- Keep your macOS updated and patched against latest vulnerabilities
- Ensure scanning all your applications even if it is being downloaded from the official App Store
- Install a reputable security product like K7 Antivirus for Mac and keep it updated to protect your device from the latest threats



Key Takeaways

The prolonged Covid-19 pandemic has taught us the necessity of remote and hybrid working schedules to keep things moving. The sudden transformation in operations also heightened security risks and challenges. Newly adopted technologies and work practices require that cybersecurity strategies be rewritten, mitigation strategies rethought, and policies stretched to be dynamic and adaptive.

Here is a quick list of tips to help you strategize your security policy for the coming days.

Enterprise

Secure your devices by keeping them up-to-date, patched against latest vulnerabilities, and protected by up-to-date, high-quality security software such as K7 Endpoint Security

Neither open documents from unknown or suspicious sources, nor enable macros in documents received from such sources

Keep your network up-to-date and patched against latest vulnerabilities

Consumer

Secure your device with a reputable security product such as K7 Total Security for Windows, K7 Antivirus for Mac and K7 Mobile Security (Android and iOS), and keep it up-to-date

Read the app's user reviews carefully before downloading and installing the same on your device

Do not install apps from unknown sources and/or third-party app stores, nor change the device settings that protects against this

K7 SECURITY

www.k7computing.com

Oct 2021